Government and the Surveillance of Private Citizens

Introduction to "Surveillance Technology"
Subcommittee on Constitutional Rights
Committee on the Judiciary, U.S. Senate
U.S. Government Printing Office
Washington, D.C. 20402

"The goals of [government] agencies are presented in attractive rhetoric; the means to achieve the ends are shrouded in secrecy; and the results are either selectively embellished for the benefit of the agency or, if unflattering, hidden from outside scrutiny. As a result, funds continue to pour into surveillance technology, and the public is stranded in a Kafkaesque muddle, unable to determine the real means and goals, the real costs and benefits."

Introduction

As every man goes through life he fills in a number of forms for the record, each containing a number of questions.... There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, busses, trams, and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence.... Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

— Alexander Solzhenitsyn, "Cancer Ward".

And if you consider that they listen around the clock to telephone conversations and conversations in my home, they analyze recording tapes and all correspondence, and then collect and compare all these data in some vast premises (and these people are not underlings), you cannot but be amazed that so many idlers in the prime of life and strength, who could be better occupied with productive work for the benefit of the fatherland, are busy with my friends and me, and keep inventing enemies.

— Alexander Solzhenitsyn, "Washington Post", April 3, 1972.

This report, although primarily targeted on the relatively narrow subject of surveillance technology, casts a broader light on social and cultural trends in modern-day America. The picture that emerges is distressing. At its worst, it shows a country at war with its own traditions, a country that fears the logic of its own charter. At its best, it shows a country beginning to grope toward an understanding of the shadowy forces threatening its uniqueness, a country beginning to define the borders beyond which technological and bureaucratic imperatives may not intrude.

From either perspective, the role of the governmental bureaucracy remains distressing. It has developed a life and rationale of its own, an organic separateness that appears anonymous and unresponsive and that often conflicts with democratic goals and with principles of good management. The bureaucracy is skillful in identifying various "threats" and "problems" and in promoting their visibility in a politically attractive way; it is far less resourceful in evaluating its own response to issues and in controlling the money and careers that quickly become vested in the perpetuation of the identified threats and problems.

These characteristics are accentuated in the agencies that contribute to the prevalence of surveillance technology. The goals of the agencies are presented in attractive rhetoric; the means to achieve the ends are shrouded in secrecy; and the results are either selectively embellished for the benefit of the agency or, if unflattering, hidden from outside scrutiny. As a result, funds continue to pour into surveillance technology, and the public is stranded in a Kafkaesque muddle, unable to determine the real means and goals, the real costs and benefits. This result is dangerous when the subject is surveillance technology, for here the marriage between technology and the growth of remote, arbitrary power is manifest. Continued ignorance of surveillance technology could prove to be an Orwellian catastrophe for privacy and freedom.

This report attempts to reduce that ignorance by bringing together in one volume the results of pertinent investigations. This report also asks a simple question: What are we doing to ourselves?

Soviet Example

In seeking answers, it may be fruitful to glance first at the Soviet Union, traditionally a negative reference point for Americans wishing to assess trends in their own society.

It takes no more than a glance to realize that personal privacy is not a highly treasured value in the Soviet Union. In their treatment of Alexander Solzhenitsyn and other political and religious dissidents, Soviet officials have made it clear that even the mildest forms of protest may cause massive intrusions into a person's private life. But the antipathy of the Soviet leadership to privacy goes far beyond specific reactions to specific irritations It is, in fact, part of their political culture, endemic to their way of life, essential to the preservation of their present political system. Invasions of privacy are viewed as necessary fixtures of everyday life, as positive components of the Soviet Union's governing ideology. Thus, all citizens, not only the Solzhenitsyns, who yearn for a measure of personal privacy will be disappointed. For example, in an editorial that appeared on March 31, 1974, "Pravda", the official Communist Party newspaper, declared that only those who are "morally untidy" worry about privacy. Not content with that, the editorial then decried "Philistine talk about one's private life allegedly being nobody's business", insisting to the contrary that "Party organizations and the public remain indifferent to instances of

Reprinted from *Surveillance Technology, Policy and Implications: An Analysis and Compendium of Materials;* staff report of the Senate Subcommittee on Constitutional Rights (Washington: U.S. Government Printing Office, 1976).

private property psychology and individualism."

Undoubtedly acting on these values, the Soviet Chamber of Commerce, acting in close cooperation with the Soviet Interior Ministry and the Soviet secret police, the KGB, invited dozens of electronics firms in the United States and other Western countries to exhibit their snooping devices at a Moscow trade fair, called Krimtekhnika '74, in August, 1974.

As the name implies, Krimtekhnika '74 was ostensibly organized to provide a forum for the exchange of technical information and sophisticated hardware in the field of law enforcement and crime control. The Soviet definition of crime, however, is rather flexible. It covers political dissent and thus includes peaceful dissenters like Alexander Solzhenitsyn, Andrei Sakharov and many others, particularly Jewish intellectuals wishing to emigrate from the Soviet Union.

Not content with learning about the criminology of distinguishing between human and animal hairs, the Soviet police officials expressed the greatest interest in viewing the products of U.S. companies that manufacture what are considered to be the world's most sophisticated voiceprint analyzers, lie detectors, identification systems, surreptitious stress analyzers, cameras for night photography and other gear designed to provide authorities with the technological means of intruding into a target's private quarters and private thoughts.

A number of U.S. companies were excited by the prospects of vast new markets for their products. Accordingly, some accepted the Soviet invitations that began circulating early in the Summer of 1974. Others had qualms. The vice president of one firm said, "Some of this equipment could be used against innocent people. It bothers me."

But nothing concerning the fair seemed to bother U.S. government officials. According to one report, an official at the Commerce Department said he had been advised on the Soviet police exhibition by the American Embassy in Moscow. "The embassy recommended that we take a hands-off position if any American businessman contacted us concerning the show," he said. As a manifestation of the government's "hands-off position", the Commerce Department initially claimed that official permission was not required for U.S. Companies to show their wares at the Moscow show.

However, when Members of Congress discovered in mid-July that American businesses, most of them heavily subsidized by government contracts, were planning to display their surveillance hardware in Moscow, there was an immediate outcry in both Houses. Senator Henry M. Jackson of Washington, whose Permanent Investigations Subcommittee of the Government Operations Committee was exploring the problems of technology transfer, said the surveillance equipment "could be used to tighten totalitarian control over minorities and dissenting intellectuals." Representative Charles A. Vanik of Ohio said that the display and sale of American surveillance technology "would be like exporting gas chambers to Hitler." Vanik recited passages from Solzhenitsyn's works to illustrate how diligently the Soviet secret police labored in the "Gulag Archipelago" to develop the very technology that was soon to be shipped to Moscow.

As a result of the intense Congressional pressure, the Nixon Administration. then in its final days (thanks in part to its efforts to use a variety of surveillance techniques against American dissenters, political opponents and reputable individuals placed on its "enemies list"), announced on July 19, 1974, the promulgation of new export restrictions to prevent Soviet police from buying sophisticated "personal surveillance" equipment. The Commerce Department said the reason for the U.S. Government's concern was "the welfare of persons who seek to exercise their fundamental rights".

The irony was probably innocent. The Krimtekhnika '74 episode in the Summer of 1974 was quickly forgotten, a brief political squall that soon passed over the horizon. But in fact the episode continues to serve as a paradigm of some of the social and political problems posed by the extraordinary growth and use of surveillance technology.

Lessons of Surveillance Fair

In the episode, for example, it is possible to see the existence of a surveillance technology industry whose principal interests lie exclusively in profit maximization and market expansion. Almost two years later, in April of 1976, a California electronics firm was, in fact, indicted for exporting $3 million in sophisticated electronics manufacturing equipment to the Soviet Union.

The episode, particularly its secret aspects, also casts light on the curious reluctance of the U.S. Government to force the Russians to halt their microwave bombardment of the American Embassy in Moscow. The bombardment is designed to interfere with American electronic eavesdropping in Moscow, but it has the unfortunate side-effect of jeopardizing the health of American personnel stationed in the Embassy. According to informed sources, the failure to force the issue is caused by the Administration's desire to avoid a detailed public airing of the highly sensitive and esoteric means by which the United States and the Soviet Union intercept important conversations within one another's borders and elsewhere around the world.

Krimtekhnika is not the only example. Shadowy government-to-government dealings in surveillance technology continue:

- In September, 1976, it was revealed that the Swedish government had secretly channeled more than $250,000 over a four-year period to the Chief of U.S. Air Force Intelligence in exchange for electronic surveillance equipment and with the apparent hope that the transaction would escape scrutiny in Sweden and that the U.S. manufacturer would believe that his goods had been sold only to the Pentagon.

- The Shah of Iran has recently signed a multi-million-dollar contract with an American company to create a communications intelligence facility in Iran capable of intercepting military and civilian communications throughout the Persian Gulf area. The contract calls for the American firm to recruit former employees of the National Security Agency and its Air Force component for the project.

- Israel is also bargaining for similar surveillance capabilities, including over-the-horizon radar, heat sensors, magnetic sensors, infrared photographic scopes, light radar scanners that can "hear" the approach of men and vehicles at distances of more than four miles and that can

estimate numbers, acoustic sensors to detect tanks or aircraft preparing for action and seismic sensors developed by the U.S. Army in Vietnam and now raised to higher levels of efficiency by the American electronics industry.

In a manner reminiscent of the arms race that began after World War II, the United States seems to be a full participant in, and even the leader of, a new competition between, and a proliferation among, the nations of the world in developing superiority in surveillance technology.

These are some international examples. As this report documents, the same made-in-America surveillance devices can be used against American citizens, with hundreds of millions in taxpayer funds poured into the research, development and dissemination of the technology of social control.

Scope and Findings of Report

This report is an effort to assess the spread of surveillance technology and to shape future investigations and discussions of the costs and benefits.

It is, emphatically, an "interim" report, for the information compiled here, as extensive as it is, can only begin to examine the vast range of issues and problems in public policymaking that fall under the rubric of surveillance technology.

As outlined on the opening day (June 23, 1975) of the series of hearings on surveillance technology held by the Subcommittee on Constitutional Rights, these issues and problems include:

> The Government's role in researching, developing, using and disseminating the technological means of invading privacy and otherwise intruding upon the constitutional rights of American citizens; the adequacy of the Government's present structures and procedures in the area of science policy for assessing the social impacts of new technology that either is designed specifically for surveillance or has derivative surveillance applications; the investment of the taxpayer's dollar to determine whether massive spending on surveillance technology has the effect of wasting scarce public funds and distorting priorities in both the public and private sectors; and the effectiveness of the administration of our present laws, and the possible need for new legislation, to regulate the growth of surveillance technology in both the public and private sectors.
>
> The investigation is unique in its scope. We will approach the problem in its entirety. We will explore the expensive, highly esoteric research and development efforts on advanced computer designs, lasers, satellites, speech processing, image enhancing and others; we will also trace the more prosaic worldwide traffic in cheap electronic eavesdropping devices and ask the responsible Government agencies about what they are doing to regulate this trade. In the process, we intend to look at the practices of Government agencies at all levels and their relationships with private industry, think tanks, and academic research centers.

It was, and remains, an ambitious undertaking. This interim report, which includes a lengthy overview of the subject, numerous texts and excerpts from relevant documents and an exhaustive bibliography, should be viewed from several perspectives: as a definitive set of findings on the structure and scope of the surveillance technology industry; as a statement of the Subcommittee's progress; as an analytic framework for informing future Congressional, Executive and public inquiries into the internal processes and external ramifications of technological advances in surveillance; and as a comprehensive research document that will stimulate and facilitate collateral studies, greater public debate and, finally, coordinated efforts to control or diminish technological threats to Constitutional liberties.

The information that supports the findings of this report has been drawn from a number of sources. The hearings and investigations of the Subcommittee on Constitutional Rights itself is a primary source of relevant information. Under the chairmanships of both Senator Sam J. Ervin, Jr., of North Carolina and Senator John V. Tunney of California, the Subcommittee has probed deeply into the mysteries and perils of computer databanks, lie detectors, wiretapping and bugging practices, military surveillance of civilians and computerized recordkeeping of intelligence files, criminal justice information systems and many other bureaucratic and technological encroachments on the traditional American concept of privacy. The long evolution of these concerns culminated in 1975 when Chairman Tunney initiated a broad series of hearings entitled "Surveillance Technology." Over the past decade many other committees in both Houses of Congress have examined in great depth various pieces of the surveillance technology puzzle. The fruits of those labors are displayed throughout this report. The extraordinary information resources of the Library of Congress give additional weight to the report's findings and recommendations. The report also borrows liberally from various documents produced by the General Accounting Office and numerous Executive Branch departments, offices, commissions and bureaus. Court opinions and other judicial and legal documents have helped to define the parameters of this report and to point to still-uncharted areas. Finally, significant data have been culled from the avalanche of articles on surveillance technology appearing in the popular and scientific press in recent years.

Yet much of this complex phenomenon remains shrouded in secrecy and jargon. Efforts to obtain authoritative information from the intelligence community are inevitably thwarted on the grounds that even the most circumspect public discussion will undermine the foundations of the Republic by revealing and thereby jeopardizing the essential "sources and methods" of the intelligence craft. The great bulk of the evidence presented in this report casts doubt on this rationale for excluding greater public understanding of the costs and benefits of surveillance technology. In addition, there are already in existence commonly accepted procedures for limited disclosure of government secrets, particularly in legal settings. Moreover, as some of the articles in this report indicate, the intelligence community is highly skilled in the selective leaking of surveillance techniques to the news media when the results are likely to prove self-promoting. Much more plausible explanations for the intelligence community's reflexive hostility toward greater public understanding of its activities are the risks of exposing still more abuses of power and corruption.

At this writing, for example, high FBI officials are being investigated for possible financial corruption involving the use of a Washington, D.C. business, U.S. Recording Co., as a front through which it channeled purchases of electronic eavesdropping equipment in order to disguise the source and nature of the

(please turn to page 8)

TO ATTACK CRITICS OF THE WARREN REPORT AROUND THE WORLD: A CIA OBJECTIVE

Associated Press

Employing "Propaganda Assets"

The Central Intelligence Agency directed its offices around the world in 1967 "to employ propaganda assets" to counter doubts raised by critics of the Warren Commission's investigation into the assassination of President Kennedy.

The propaganda campaign was to be waged in part by passing unclassified information about the assassination to CIA "assets" who could use the material in writing "book reviews and feature articles" that would "answer and refute the attacks of the critics" according to a newly released CIA document.

"To Discredit the Claims of Conspiracy Theorists"

The document said the aim was "to provide material for countering and discrediting the claims of the conspiracy theorists, so as to inhibit the circulation of such claims in other countries."

The document was among some 850 pages of material released yesterday by the CIA under the Freedom of Information Act.

The Documents show that the CIA examined copies of almost all books about the November, 1963, assassination, including one by then-Congressman Gerald R. Ford.

Gerald Ford's Book Using Secret Session Material

A CIA officer called Ford's book "a re-hash of the Oswald case" and criticized its "loose" writing.

Ford was a member of the Warren Commission which concluded that Lee Harvey Oswald was solely responsible for the assassination. Ford quoted extensively from secret sessions of the commission in his book, "Portrait of an Assassin", which agreed with the commission's finding.

"Casting Doubt on the Whole Leadership of American Society"

The 1967 dispatch to "chiefs, certain stations and bases" says that the rash of books and articles criticizing the Warren Commission's finding "is a matter of concern to the U.S. government, including our organization.

"Efforts to impugn [the] rectitude and wisdom [of commission members and staff] tend to cast doubt on the whole leadership of American society," the memo said.

"Moreover, there seems to be an increasing tendency to hint that President Johnson, himself, as the one person who might be said to have benefited, was in some way responsible for the assassination.

"Our Ploy Should Point Out..."

"Innuendo of such seriousness affects not only the individual concerned, but also the whole reputation of the American Government."

In using propaganda assets to refute these charges, the dispatch said, "our ploy should point out, as applicable, that the critics are (1) wedded to theories adopted before the evidence was in, (2) politically interested, (3) financially interested, (4) hasty and inaccurate in their research, or (5) infatuated with their own theories." □

(Based on a report "Critics of Warren Report Objects of CIA Campaign" in a Washington Newspaper, February 1977 — reference not available currently, but will be published.)

Surveillance — *Continued from page 7*

equipment. The question under investigation is whether, because of close personal relationships between the head of the electronics firm and FBI leaders, the company had enjoyed an unfair edge in obtaining the FBI's business, or had been allowed to charge unreasonably high markups for its services or had kicked back money or favors to the FBI personnel. Justice Department officials believe the risks of corruption are high in the area of intelligence, where the law, for reasons of security, allows the intelligence community great latitude in negotiating fees and giving out contracts without competitive bids. Fear of embarrassment and a showing of incompetence may also lie behind the rigid hostility to public scrunity. And finally, as noted before, the intelligence community is undoubtedly worried about the political consequences of disclosing more information about the extent to which it already enjoys the technological ability to destroy the privacy of innocent American citizens.

Despite the obstacles created by the attitude of the intelligence community, the documents in this report represent in their entirety an instrument by which researchers may tringulate the major themes and activities that result from the intelligence community's commitment to technological surveillance. Thus, although the reasoning that leads to the findings and recommendations of this report may in some instances be more deductive than inductive, the conclusions are all firmly rooted in the documents and references contained in the report.

The findings of this report are hardly reassuring. The report finds that:

- there is indeed a surveillance technology industry;
- the industry is largely unregulated and unscrutinized and, as a result, poses a serious threat to the privacy, liberty and security of every American;
- The key factor determining the continued worldwide growth of the industry is the formal and informal support of the surveillance bureaucracies within the Executive Branch of the Federal Government;
- the Federal Government fails to articulate a coherent national policy on surveillance technology, fails to assess the social, political and economic impact of surveillance technology, and thus fails to provide even rudimentary controls;
- the Congress is precluded from effective oversight of the expenditure of public tax monies in support of the surveillance technology industry by the systematic and pervasive secrecy that cloaks important aspects of its operations;
- new institutional mechanisms need to be developed within the Congress and the Executive Branch to redress the growing imbalance between governmental power based on the technology of surveillance and the Constitutional rights of individual American citizens.

(To be continued in next issue)